Algebraic Characterization of the Class of Languages recognized by Measure Only Quantum Automata

Carlo Comin *
Dipartimento di Informatica,
Universitá degli Studi di Milano
via Comelico 39/41, Milano, Italy.
carlo.comin@studenti.unimi.it

January 29, 2013

Abstract

We study a model of one-way quantum automaton where only measurement operations are allowed (MON-1QFA). We give an algebraic characterization of $\mathbf{LMO}(\Sigma)$, showing that the syntactic monoids of the languages in $\mathbf{LMO}(\Sigma)$ are exactly the J-trivial literally idempotent syntactic monoids, where J is the Green's relation determined by two-sided ideals. We also prove that $\mathbf{LMO}(\Sigma)$ coincides with the literal variety of literally idempotent piecewise testable regular languages. This allows us to prove the existence of a polynomial time algorithm for deciding whether a regular language belongs to $\mathbf{LMO}(\Sigma)$ and to discuss definability issues in terms of the existential first-order logic $\Sigma_1[<]$ and the linear temporal logic without the next operator LTLWN.

1 Introduction

This paper gives a characterization of the class of languages recognized by a model of quantum automata, by using tools from algebraic theory, in particular, varieties of languages and syntactic monoids. Many models of one-way quantum finite automata are present in the literature: the oldest is the Measure-Once model [3, 7], characterized by unitary evolution operators and a single measurement performed at the end of the computation. On the contrary, in other

*The author wish to thank Prof. Alberto Bertoni for having introduced him to the problem and for the stimulating discussions and research directions that finally lead to the results of this paper, Dr. Maria-Paola Bianchi for the kind collaboration on the structural drawing-up of the article.

models, evolutions and measurements alternate along the computation [1, 17]. The model we study is the Measure-Only Quantum Automaton (MON-1QFA), introduced in [5], in which we allow only measurement operations, not evolution. All these quantum models are generalized by Quantum Automata with Control Language [4]. We also remind that the use of quantum measurements as computational steps is an active area of research, falling under the umbrella-name of MBQC (measurements-based quantum computation); we cite for instance the teleportation based model and the one-way quantum computer of cluster state computation [12, 18, 19].

Originally, the MON-1QFA model has been introduced by *Alberto Bertoni, et al.*, upon the framework of trace theory and free partial commutative monoids [5, 2, 8], giving evidence that *Giancarlo Mauri*'s approach to link trace theory to that of free partially commutative monoids can be useful also in the area of *quantum computing*. Those insights finally lead to the results contained in [5], in which the authors proved that every formal series induced by the probabilistic behaviour of a MON-1QFA admits a linear representation with projectors, moreover, that the whole family of such formal series is closed under f-complement and Hadamard product and, as a main result, that the class of languages recognized by MON-1QFAs over compatibility alphabets (Σ, E) is a boolean algebra of recognizable languages with finite variation.

Here we study MON-1QFAs over classical alphabets Σ, thus relaxing the requirement which forces us to fix a compatibility relation E. We shall denote the class of formal languages recognized by MON-1QFAs over Σ as $\mathbf{LMO}(\Sigma)$. By doing so we study a super-class of the languages studied in [5] and prove a characterization result in terms of the properties satisfied by syntactic monoids of those languages; in particular we lean upon the notion of J-triviality (where J is one of the Green's relation, determined by two-sided monoid ideals) and the literal idempotency relation, i.e. $\sigma^2 \sim \sigma$ for every $\sigma \in \Sigma$. This general approach, to study properties of formal languages as a reflex-effect of the algebraic properties and equations satisfied by their syntactic monoids, is a well-established and celebrated principle in the algebraic theory of automata and formal languages, having roots in finite semigroup and finite monoid theory. The pillars of the formerly mentioned algebraic framework stand in the seminal works of *Eilenberg*, *Shützenberger*, *Simon*, *Straubing*, *Pin*, et al.; for instance, we would like to cite it here the celebrated *Variety Theorem* of Eilenberg [9], the algebraic characterization of the piecewise testable languages in terms of J-trivial syntactic monoids given by Simon [21], the algebraic characterization of the star-free languages by means of aperiodic syntactic monoids of Shützenberger and the broad algebraic theory of varieties of languages and pseudovarieties of monoids developed by Straubing, Pin, et al. [20]. Indeed, those powerful algebraic masterworks have been already used successfully in order to characterize classes of languages recognized by finite-state quantum devices; as in the work of *Ambainis, et al.* [1], in which the authors established intimate ties between the class of so-called *Latvian* automata and the pseudovariety $\mathbf{BG}$ of block-group syntactic

monoids.

As an aftermath of our mathematical journey, with this work we stand to defend that a formal language L is recognized by some MON-1QFA if and only if it is a literal idempotent piecewise testable language, that is, if and only if its syntactic monoid is J-trivial and it is such that its associated syntactic homomorphism literally satisfies the idempotency pseudoidentity $x^2 = x$; this particular literal variety of the literally idempotent regular languages has been already studied algebraically by Klíma and Polák in [15]. As a corollary, we solve the polynomial-time decidability question for **LMO** in the affirmative direction by proving the existence of a polynomial-time algorithm for deciding whether a regular language belongs to $\mathbf{LMO}(\Sigma)$. We also discuss the definability of languages recognized by MON-1QFAs in terms of *easy* formulas of the existential first-order logic $\Sigma_1[<]$ and *easy* formulas of the linear temporal logic without the next operator LTLWN. We would like to remind that the logical approach to automata and formal languages is also a well-established area of mathematical research, pioneered by the work of *Büchi* [6]; to the best of our knowledge, he was the first to conceive and prove that the regular languages are exactly those languages definable in the monadic second-order logic.

We shall see and highly remark that it is an extremely beauty asset of automata and formal language theory to be a bridge between quantum, algebraic and logical insights.

2 Preliminaries

2.1 Notation

We shall denote by $\mathbb{N} := \{0, 1, 2, \cdots\}$ the set of natural numbers and by $\mathbb{N}_0 := \{1, 2, \cdots\}$ the set of the positive ones. A semigroup is any set S together with a binary operation $\cdot$ that is associative. A monoid M is a semigroup containing an identity element 1_M. If S is a semigroup with no identity, we denote by S^1 the monoid obtained by $S \cup \{1_M\}$ such that 1_M is an identity in S. If S is a monoid, then $S^1 = S$. If S, S' (M, M') are semigroups (monoids), and the map $\varphi : S \to S'$ $(\varphi : M \to M')$ it is such that $\varphi(x \cdot x') = \varphi(x) \cdot \varphi(x')$ for every $x \in S$ $(x \in M)$, then we say that φ is a semigroup (monoid) homomorphism; we denote by $\varphi : X \hookrightarrow Y$ injective homomorphisms, by $\varphi : X \twoheadrightarrow Y$ surjective and by $\varphi : X \leftrightarrow Y$ bijective homomorphisms.
Given a finite alphabet Σ, we write Σ^* to denote the free monoid generated by Σ. The free monoid Σ^* includes all possible words whose letters belong to Σ and the empty word ϵ. If $w \in \Sigma^*$ is a word, we denote its length by $|w|$ and its letters by $w_1, \dots, w_n$. If $L \subseteq \Sigma^*$ is a subset of Σ^*, then we say that L is a formal language. A deterministic finite state automaton is a tuple $A := \langle \Sigma, Q, \delta, q_0, F \rangle$ where $\delta : \Sigma \times Q \to Q$ is called the transition function of A and $L_A := \{w \in \Sigma^* | \delta(w) \in F\}$ (where $\delta(w) := \delta(\cdots \delta(\delta(q_0, w_1), w_2), w_n)$ for

any $w := w_1 \cdots w_n, |w| = n$) is the language recognized by A. If L is recognized by a finite state automaton, then we say that L is regular.
Let L be a regular language and let $A_L := \langle \Sigma, Q, \delta, q_0, F \rangle$ be the minimal deterministic automaton recognizing L. For any word $w = w_1 \cdots w_n \in \Sigma^*$, we define its variation as the cardinality $\mathrm{var}_L(w) := \#\{0 \leq k < n \mid \delta(w_1 \cdots w_k) \neq \delta(w_1 \cdots w_{k+1})\}$. We say that L has *finite variation* if and only if $\sup_{x \in \Sigma^*} \mathrm{var}_L(x) < \infty$.

2.2 Linear algebra for quantum systems

In this section we briefly outline some notions of linear algebra in order to describe the concepts of quantum observable, quantum measurement and, more generally, quantum finite-state computing device. This brief summary follows the one given in [5]. We denote the field of complex numbers by $\mathbb{C}$. Given a complex number $z \in \mathbb{C}$, its complex conjugate is denote by z^*, and its modulus by $|z| = \sqrt{zz^*}$. We denote by $\mathbb{C}^{m \times n}$ the set of $m \times n$ matrices with complex valued entries. For any $M \in \mathbb{C}^{m \times n}$ and for any $1 \leq i \leq m$ and $1 \leq j \leq n$, we denote by M_{ij} or $(M)_{ij}$ the (i, j)-th entry of M. The *adjoint matrix* of $M \in \mathbb{C}^{m \times n}$ is denoted by $M^\dagger$ and is defined by $M^\dagger = (M^*)^T = (M^T)^*$, provided that M^* is defined by $M^*_{ij} := (M_{ij})^*$. The *trace* of a square matrix $M \in \mathbb{C}^{n \times n}$ is defined as $\mathrm{Tr}(M) := \sum_{i=1}^n M_{ii}$. If $A, B \in \mathbb{C}^{m \times n}$ then their sum is the $m \times n$ matrix whose (i, j)-entry is given by $(A + B)_{ij} = A_{ij} + B_{ij}$. If $C \in \mathbb{C}^{m \times n}$ and $D \in \mathbb{C}^{n \times p}$, their product is the $m \times p$ matrix whose (i, j)-entry is given by $(AB)_{ij} = \sum_{k=1}^n C_{ik} D_{kj}$. If $A \in \mathbb{C}^{m \times n}$ and $B \in \mathbb{C}^{p \times q}$ then their direct sum and Kronecker (or direct) product are the $(m + p) \times (n + q)$ and $mq \times nq$ matrices defined, respectively, as follows:

$$A \oplus B := \begin{pmatrix} A & \mathbf{0} \\ \mathbf{0} & B \end{pmatrix} \quad A \otimes B := \begin{pmatrix} A_{11}B & \cdots & A_{1n}B \\ \vdots & \ddots & \vdots \\ A_{m1}B & \cdots & A_{mn}B \end{pmatrix}$$

where $\mathbf{0}$ denotes null matrices of suitable dimensions. Provided that matrices dimensions allow to perform operations, it holds $(A \otimes B)(C \otimes D) = AC \otimes BD$. An Hilbert space of finite dimension m is the linear space $\mathbb{C}^{1 \times m}$ equipped with sum and product by elements in $\mathbb{C}$, in which the *inner product* is defined as $(\pi, \xi) := \pi \xi^\dagger$. If $(\pi, \xi) = 0$ then we say that π is *orthogonal* to ξ. The norm of vector π is given by $||\pi|| := \sqrt{(\pi, \pi)}$. Two subspaces X, Y are orthogonal if any vector in X is orthogonal to any vector in Y and, in this case, the linear space generated by $X \cup Y$ is denoted by $X \oplus Y$. A matrix $M \in \mathbb{C}^{m \times m}$ can be view as a morphism $\pi \mapsto \pi M$ of the Hilbert space $\mathbb{C}^{1 \times m}$ in itself and it is said Hermitian whenever $M = M^\dagger$. Given an Hermitian matrix O, we denote by $\lambda_1, \ldots, \lambda_s$ its eigenvalues and $E_1, \ldots, E_s$ the corresponding eigenspaces. It is well-known that each eigenvalue λ_k is real, that E_i is orthogonal to E_j for any $i \neq j$ and that $E_1 \oplus \cdots \oplus E_s = \mathbb{C}^{1 \times m}$. Each vector π can be uniquely decomposed as $\pi = \pi_1 + \cdots + \pi_s$, where $\pi_j \in E_j$; the linear transformation $\pi \mapsto \pi_j$ is called projector P_j on the subspace E_j. A linear operator is a projector

if and only if it is Hermitian and idempotent. Every Hermitian matrix O is uniquely determined by its eigenvalues and its eigenspaces, or by its projectors. By the spectral decomposition theorem it holds that, for some $s \in \mathbb{N}_0$, $O = \sum_{i=1}^{s} \lambda_i P_i$ and we denote by $V(O) := \{\lambda_i\}_{i=1}^{s}$ the spectrum of O. Given two Hermitians $O_1 := \sum_{i=1}^{s} \lambda_i P_i$ and $O_2 := \sum_{i=1}^{t} \mu_i Q_i$ it is always possible to find new eigenvalues and Hermitian operators such that $O_1' = \sum_{i=1}^{s} \lambda_i' P_i, O_1' = \sum_{i=1}^{s} \mu_i' Q_i$ and $V(O_1' \otimes O_2') = V(O_1) \times V(O_2)$. Given a set $e_1, \ldots, e_m$ of pure states, a *quantum state* is a superposition $\pi = \sum_{k=1}^{m} \pi_k e_k$ where the coefficients π_k are complex *amplitudes* and $||\pi|| = 1$. A *quantum observable* is represented by an Hermitian operator $O = \sum_{i=1}^{s} \lambda_i P_i$ where $V(O)$ is the set of possible results of a measurement of O. A measurement of O on π will return λ_j with probability $||\pi P_j||^2$ and the state after the quantum measurement becomes $\pi P_j / ||\pi P_j||^2$.

2.3 Varieties of formal languages, pseudovarieties of finite monoids, literal idempotency

This section is devoted to the recall of some general definitions and results from the algebraic theory of automata and formal languages. For more details, we refer the reader to, e.g. [9, 20].

Definition 1 (Syntactic monoid)**.** *Let $L \subseteq \Sigma^*$ be a language over the alphabet Σ. We shall define the syntactic congruence $\sim_L$ w.r.t. L as follows: for every $x, y \in \Sigma^*$, $x \sim_L y$ if and only if for every $a, b \in \Sigma^*$ it holds that $axb \in L \iff ayb \in L$. For any language $L \subseteq \Sigma^*$, we call the quotient monoid $M(L) := \Sigma^* / \sim_L$ the* syntactic monoid *of L.*

Definition 2 (M-pseudovariety)**.** *We say that a class of finite monoids $\mathbf{M}$ is a* pseudovariety *if and only if the following three conditions holds: (i) If $M \in \mathbf{M}$ and N is a submonoid of M, then $N \in \mathbf{M}$. (ii) $M \in \mathbf{M}$ and Q is a homomorphic image, i.e. quotient monoid, of M, then $Q \in \mathbf{M}$. (iii) If $M, N \in \mathbf{M}$, then the direct product monoid $M \times N$ is also in $\mathbf{M}$.*

Definition 3 (Literal pseudovariety [15])**.** *Let $\mathbf{H}$ be a class of surjective homomorphisms from free monoids over non-empty sets onto finite monoids. Then $\mathbf{H}$ is a* literal pseudovariety *if it is closed with respect to the homomorphic images, literal substructures and products of finite families; more precisely, the following three conditions must be satisfied: (i) For each $(\phi : \Sigma^* \twoheadrightarrow M) \in \mathbf{H}$ and surjective monoid homomorphism $\sigma : M \twoheadrightarrow N$, it holds $\sigma\varphi \in \mathbf{H}$. (ii) For each $(\phi : \Sigma^* \twoheadrightarrow M) \in \mathbf{H}$ and for each free monoid homomorphism $f : \Gamma^* \to \Sigma^*$ such that $f(\Gamma) \subseteq \Sigma$, it holds $(\varphi f : \Gamma^* \twoheadrightarrow (\varphi f)(\Gamma^*)) \in \mathbf{H}$. (iii) For each non-empty set Σ, the mapping of Σ^* onto the one element monoid $\{1\}$ is in $\mathbf{H}$, moreover, for each $\varphi : \Sigma^* \twoheadrightarrow M, \psi : \Sigma^* \twoheadrightarrow N$, the natural homomorphism of Σ^* onto $\Sigma^* / (ker\, \varphi \cap ker\, \psi)$ is in $\mathbf{H}$.*

Definition 4 (*-variety and literal variety of languages)**.** *Let $\mathbf{M}$ be a class of monoids and let Σ be an alphabet. We denote by $V_\Sigma(\mathbf{M})$ the class of regular languages on Σ having syntactic monoid in $\mathbf{M}$. We say that a class of regular*

languages $V : \Sigma \to 2^{\Sigma^*}$ is a $*$-variety of Eilenberg *if V is closed under boolean operations, right and left quotient, and inverse homomorphism. Replacing closure under inverse homomorphism by closure under inverse literal homomorphism, we get the notion of literal variety of languages. More precisely, closure under literal homomorphisms holds whenever the following condition is satisfied: for each alphabets Γ and Σ and a free-monoid homomorphism $f : \Gamma^* \to \Sigma^*$ such that $f(\Gamma) \subseteq \Sigma$, $L \in V(\Sigma)$ implies $f^{-1}(L) \in V(\Gamma)$.*

A fundamental result is due to Eilenberg, who showed that there exists a bijection V from the psuedovarieties of monoids and the $*$-varieties of Eilenberg of formal languages [20]. This result has been extended in literature in many ways; for instance, Straubing considered the more general notion of $\mathbb{C}$-variety [22] and the work of Ésik, et.al. [10], [11] focused on literal varieties and the corresponding links with literal pseudovarieties. Due to Kunc [16] we also have equational logic for those classes of languages. The following result of Eilenberg is thus prominent and of remarkable importance in the algebraic theory of automata and formal languages.

Theorem 1 (Eilenberg's Variety Theorem [20])**.** *Let $\mathbf{V}$ be a pseudovariety of monoids and let Σ be an alphabet. We denote by V_Σ the set of recognizable languages of Σ^* whose syntactic monoid is within $\mathbf{V}$. The map*

$$\mathbf{V} \to V$$

allows us to associate with each variety of monoids a class of recognizable languages. Morover, it establishes a bijection from the psuedovarieties of monoids and the $*$-varieties of Eilenberg of formal languages.

We also recall some fundamental equivalence relations studied by Green in 1951. They allow us to describe some $*$-varieties of languages arising from the notion of *triviality* with respect to Green's equivalence classes. For instance, we introduce the pseudovariety of J-trivial monoids and the $*$-variety of the piecewise testable languages defined below.

Definition 5 (Green's relations)**.** *We denote by L, R and J the Green's relations determined by left, right and two-sided ideals, respectively. In more detail, let S be a semigroup, for any $a, b \in S^1$ we have*

(i) $aLb \iff S^1a = S^1b$.

(ii) $aRb \iff aS^1 = bS^1$.

(iii) $aJb \iff S^1aS^1 = S^1bS^1$.

Let S be a semigroup and K be one of Green's relations, we say that S is K-trivial if and only if aKb implies $a = b$, for every $a, b \in S$. In this paper we denote by $\mathbf{R}$ the pseudovariety of R-trivial finite monoids and by $\mathbf{J}$ the pseudovariety of J-trivial finite monoids. We also define $\overline{\mathbf{J}}$ as the class of J-trivial finite monoids M such that every surjective homomorphism $\varphi : \Sigma^* \twoheadrightarrow M$ from the free monoid generated by a non-empty set onto M literally satisfies the idempotency pseudoidentity $x^2 = x$, i.e. $\varphi(\sigma)\varphi(\sigma) = \varphi(\sigma)$, for every $\sigma \in \Sigma$.

Definition 6 (Literally idempotent piecewise testable languages)**.** *We say that a language $L \in \Sigma^*$ is literally idempotent if and only if for all $x, y \in \Sigma^*$ and $a \in \Sigma$, $xa^2y \in L \Leftrightarrow xay \in L$. We say that L is a piecewise testable language if and only if it lies in the boolean closure of the following class of languages, defined for each $k \geq 0$:*

$$\Sigma^* a_1 \Sigma^* a_2 \Sigma^* \cdots \Sigma^* a_k \Sigma^*, \text{ for } a_1, a_2, \ldots, a_k \in \Sigma$$

Moreover, we say that L is literally idempotent piecewise testable if and only if it lies in the boolean closure of the following class of languages, defined for each $k \geq 0$:

$$\Sigma^* a_1 \Sigma^* a_2 \Sigma^* \cdots \Sigma^* a_k \Sigma^*, \text{ for } a_1, a_2, \ldots, a_k \in \Sigma \text{ and } a_i \neq a_{i+1} \text{ for every } 1 \leq i < k$$

*We denote by **PT** the class of piecewise testable languages. We denote by liId the class of literally idempotent languages and by liId**PT** the class of literally idempotent piecewise testable languages.*

One of the first known instances of the Eilenberg Variety Theorem is based on the J relation. It has been proved by Simon the following remarkable characterization result:

Theorem 2 (Simon, [21])**.** *L is a piecewise testable language if and only if its syntactic monoid is J-trivial.*

In [15], Klíma and Polák showed the following characterization result for the literally idempotent piecewise testable languages.

Theorem 3 (Klíma, Polák, [15])**.** *Let $L \subseteq \Sigma^*$ be a formal language. The following propositions are equivalent:*

(i) L lies in the boolean closure of the following class of languages:
$\Sigma^* a_1 \Sigma^* a_2 \Sigma^* \cdots \Sigma^* a_k \Sigma^*$ for $a_1, a_2, \ldots, a_k \in \Sigma$ and $a_i \neq a_{i+1}$ for every $1 \leq i < k$,
that is to say $L \in liId\boldsymbol{PT}$.

(ii) L is picewise testable and literally idempotent, that is to say $L \in \boldsymbol{PT} \cap liId(\Sigma) = V_\Sigma(\mathbf{J}) \cap liId(\Sigma)$.

(iii) the syntactic monoid of L is J-trivial and satisifies the pseudoidentity $\sigma^2 = \sigma$ literally,
we denote this fact by $L \in V_\Sigma\left(\overline{\mathbf{J}}\right)$.

3 Measure Only Quantum Automata over Σ

In this section we introduce and begin to analyse the model of MON-1QFAS, that is our main object of study in this work.

Definition 7 (MON-1QFA over Σ)**.** *A* MON-1QFA *over the alphabet* Σ *is a tuple of the form* $A := \langle \Sigma \cup \{\#\}, (O_c)_{c\in\Sigma\cup\{\#\}}, \pi_0, F\rangle$*. The complex* m*-dimensional vector* $\pi_0 \in \mathbb{C}^{1\times m}$*, with unitary norm* $||\pi_0|| = 1$*, is called the quantum initial state of* A*. For every* $c \in \Sigma$*,* $O_c \in \mathbb{C}^{m\times m}$ *is (the representative matrix of) an idempotent Hermitian operator and denotes an observable. The subset* $F \subseteq V(O_\#)$ *of the eigenvalues of* $O_\#$ *is called the spectrum of the quantum final accepting states of* A*. We also say that* A *is of finite dimension* $m \in \mathbb{N}_0$*.*

Indeed, the MON-1QFA model has been originally introduced in the context of free partial commutative monoids with idempotent generators [5]. Let (Σ, E) be a *compatibility alphabet*, that is a finite simple graph over a finite non-empty set Σ. Let us denote by $\underline{E}$ the least congruence containing (cc, c) for all $c \in \Sigma$ and (ab, ba) for all $a, b \in \Sigma$ such that $(a, b) \in E$. We say that $\Sigma^*/\underline{E}$ is a *free partially commutative monoid with idempotent generators* and we denote it by $\mathrm{FI}(\Sigma, E)$. Each element $t \in \mathrm{FI}(\Sigma, E)$, that is an equivalence class of $\underline{E}$, shall be seen as a language $t \subseteq \Sigma^*$.
Following the same path of Definition 7, a MON-1QFA over the compatibility alphabet (Σ, E) is a tuple of the form $A := \langle(\Sigma, E) \cup \{\#\}, (O_c)_{c\in\Sigma\cup\{\#\}}, \pi_0, F\rangle$ where the complex m-dimensional vector $\pi_0 \in \mathbb{C}^{1\times m}$, with unitary norm $||\pi_0|| = 1$, is called the quantum initial state of A and for every $c \in \Sigma$, $O_c \in \mathbb{C}^{m\times m}$ is (the representative matrix of) an idempotent Hermitian operator and denotes an observable. Also, the subset $F \subseteq V(O_\#)$ of the eigenvalues of $O_\#$ is called the spectrum of the quantum final accepting states of A.

In the specific case of MON-1QFAs over Σ, the computation dynamics of automaton A is carried out in the following way: let $w = w_1 \ldots w_n \in \Sigma^*$, suppose we start from π_0, then A measures the system with cascade observables $O_{w_1}, \ldots, O_{w_n}$ (by applying the associated orthogonal projectors) and then performs the final measure with the end-word observable $O_\#$, that is, the observable of the final accepting states F of A.
This last measure returns, as a result, an eigenvalue $r_j \in V(O_\#)$, if $r_j \in F$ then we say that the automaton A accepts the word $w \in \Sigma^*$, otherwise that A does not accept it. What is remarkable in this computation dynamics, is the *probabilistic behavior* of the automaton A, that is, the probability $p_A(w)$ that A accepts $w = w_1 \cdots w_n$. We say that a language L is recognized by A with *isolated cut point* $\lambda \in \mathbb{R}$ if and only if, for all $w \in \Sigma^*$ it holds that $p_A(w) > \lambda \Leftrightarrow w \in L$ and there exists a constant value $\delta > 0$ such that for all $w \in \Sigma^*$ it holds that $|p_A(w) - \lambda| \geq \delta$.

This computing behaviour can be actually made more formal, it turns out to be of some interest to express $p_A(w)$ using the well-known formalism of quantum density matrices; we divert the reader to [13] for a general treatise.

Definition 8. *Let* $x \in \Sigma^*$ *be a word over the alphabet* Σ*. Let* $A := \langle \Sigma \cup \{\#\}, (O_c)_{c\in\Sigma\cup\{\#\}}, \pi_0, F\rangle$ *be a* MON-1QFA *over* Σ *such that, for each* $c \in \Sigma$*, the observable* O_c *admits the following spectral decomposition* $O_c = \sum_{j=1}^{k(c)} \lambda_j P_j(c)$*; where* $k(c)$ *is the cardinality of the spectrum of* O_c*. Then, we shall define the*

quantum density matrix $\sigma_A(x) \in \mathbb{C}^{m\times m}$ *of* x *w.r.t.* A *as follows:*

$$\sigma_A(x) = \begin{cases} \pi_0^\dagger \pi_0 & \text{if } x = \epsilon \\ \sum_{j=1}^{k(c)} P_j(c)\sigma(y)P_j(c) & \text{if } x = yc \text{ for } c \in \Sigma \text{ and } k(c) \text{ is the} \\ & \text{number of projectors } P_j \text{ decomposing } O_c \end{cases}$$

Definition 9. *Let* $x \in \Sigma^*$ *be a word over the alphabet* Σ. *Let* $A := \langle \Sigma \cup \{\#\}, (O_c)_{c\in\Sigma\cup\{\#\}}, \pi_0, F\rangle$ *be a* MON-1QFA *over* Σ *and let* $\sigma_A(x)$ *be the quantum density matrix of* x *w.r.t.* A. *Then, we shall formally define the probabilistic behaviour* $p_A(x)$ *of* x *w.r.t.* A *as follows:*

$$p_A(x) := Tr\left(\sum_{r_j\in F} P_{r_j}(\#)\sigma_A(x)P_{r_j}(\#)\right)$$

provided that r_j *goes among the projectors of* $O_\#$ *that are in* F *only.*

Proposition 1. *Let* $A := \langle \Sigma\cup\{\#\}, (O_c)_{c\in\Sigma\cup\{\#\}}, \pi^A, F^A\rangle$ *be a* MON-1QFA *over* Σ^* *such that, for every* $c \in \Sigma$, O_c *admits the following spectral decomposition* $O_c = \sum_{j=1}^{k(c)} \lambda_j P_j(c)$. *Then, for every* $w \in \Sigma^*$ *such that* $w := w_1 \cdots w_n$ *and such that* $k(w_i)$ *is the cardinality of the spectrum of* O_{w_i} *for each* $1 \le i \le n$, *the probabilistic behaviour* $p_A(w)$ *of* w *w.r.t.* A *is given by the following expression:*

$$p_A(w) = \sum_{r_j\in F}\sum_{j_1,\ldots,j_n} ||\pi_0 P_{j_1}(w_1)\cdots P_{j_n}(w_n)P_{r_j}(\#)||_2^2$$

provided that, for every $1 \le i \le n$, j_i *goes from* 1 *to* $k(w_i)$ *and provided that* r_j *goes among the projectors of* $O_\#$ *that are in* F *only.*

Proof. Let $x := x_1 \cdots x_n \in \Sigma^*$, apply induction on n and the properties that $P^\dagger = P$ for every Hermitian P and $(AB)^\dagger = B^\dagger A^\dagger$ for every operator A and B. Then the following holds.

$$\begin{aligned} p_A(x) &= \mathrm{Tr}\left[\sum_{r_j\in F} P_{r_j}(\#)\sigma(x)P_{r_j}(\#)\right] \\ &= \mathrm{Tr}\Big[\sum_{r_j\in F} P_{r_j}(\#)\Big(\sum_{j_n=1}^{k(x_n)} P_{j_n}(x_n)\Big(\\ &\qquad \sum_{j_{n-1}=1}^{k(x_{n-1})} P_{j_{n-1}}(x_{n-1})(\cdots\pi_0^\dagger\pi_0\cdots)P_{j_{n-1}}(x_{n-1})\Big)P_{j_n}(x_n)\Big)P_{r_j}(\#)\Big] \\ &= \mathrm{Tr}\Big[\sum_{r_j\in F}\sum_{j_n=1}^{k(x_n)}\cdots\sum_{j_1=1}^{k(x_1)} \\ &\qquad P_{r_j}^\dagger(\#)P_{j_n}^\dagger(x_n)P_{j_{n-1}}^\dagger(x_{n-1})\cdots P_{j_1}^\dagger(x_1)\pi_0^\dagger\pi_0 P_{j_1}(x_1)\cdots P_{j_{n-1}}(x_{n-1})P_{j_n}(x_n)P_{r_j}(\#)\Big] \\ &= \mathrm{Tr}\Big[\sum_{r_j\in F}\sum_{j_n=1}^{k(x_n)}\cdots\sum_{j_1=1}^{k(x_1)} \\ &\qquad (\pi_0 P_{j_1}(x_1)\cdots P_{j_{n-1}}(x_{n-1})P_{j_n}(x_n)P_{r_j}(\#))^\dagger(\pi_0 P_{j_1}(x_1)\cdots P_{j_{n-1}}(x_{n-1})P_{j_n}(x_n)P_{r_j}(\#))\Big] \end{aligned}$$

Observe that for every $a \in \mathbb{C}^{1\times m}$ and $1 \le i \le m$ it holds that $(a^\dagger a)_{i,i} = a_i^* a_i$. Then $\mathrm{Tr}(a^\dagger a) = ||a||_2^2$. The thesis follows. $\square$

Proposition 2. *The formal power series generated by a* MON-1QFA A *on* Σ *with* m *states admits a linear representation* $\langle \xi, (P(c))_{c\in\Sigma}, \eta\rangle$ *where* $||\xi|| = 1$, $P(c)$ *is a projector for all* $c \in \Sigma$ *and* $||\eta|| \leq \sqrt{m}$.

Proof. The proof is almost identical to the one given over (Σ, E) in [5]. See Appendix A. $\square$

Proposition 3. *The class* $\boldsymbol{PMO}(\Sigma)$ *is closed under the operations of Hadamard product and* f*-complement.*

Proof. The proof is almost identical to the one given over (Σ, E) in [5]. Se Appendix A. $\square$

Proposition 4. *Let* $L \in \boldsymbol{LMO}(\Sigma)$ *and* χ_L *be its characteristic function. For any* $\epsilon > 0$, *there exists* $\phi \in \boldsymbol{PMO}(\Sigma)$ *such that* $|\phi(w) - \chi_L(w)| < \epsilon$, *for all* $w \in \Sigma^*$.

Proof. The proof is almost identical to the one given over (Σ, E) in [5]. See Appendix A. $\square$

Lemma 1. *Given a formal series* $\phi : \Sigma^* \to [0, 1]$, *let* $\langle \xi, (P(c))_{c\in\Sigma}, \eta\rangle$ *be a linear representation of* ϕ, *where* $||\xi|| = 1$ *and* $P(c)$ *is a projector for* $c \in \Sigma$, $P(\epsilon) = I$. *Suppose that* $|\phi(w)-\lambda| \geq \delta > 0$ *for all* $w \in \Sigma^*$, *and let* $L := \{w \in \Sigma^* | \phi(w) > \lambda\}$.

(i) T *is a regular language on* Σ^*.

(ii) there exists a finite state automaton $\langle \Sigma, Q, (\underline{\delta}_c)_{c\in\Sigma}, q_0, F\rangle$ *recognizing* L *such that, for any* $w, u \in \Sigma^*$, *the following holds:* $\underline{\delta}_w(q_0) \neq \underline{\delta}_u(q_0)$ *implies* $||\xi P(w) - \xi P(u)|| \geq \frac{\delta}{||\eta||}$.

Proof. The proof technique is classical and it is almost identical to the one given in [5] for formal series over FI(Σ, E). We included it in Appendix A. $\square$

Lemma 2. *Let* Σ *be a finite non-empty set. The class* $\boldsymbol{LMO}(\Sigma)$ *is closed under intersection, complement and union.*

Proof. The proof is almost identical to the one given over (Σ, E) in [5]. See Appendix A. $\square$

Proposition 5. $\boldsymbol{LMO}(\Sigma)$ *is a boolean algebra of regular languages in* Σ^* *with finite variation. In particular, if* L *is a language recognized by a* MON-1QFA *over* Σ *with* m *states and isolation* δ, *then* $\sup_{x\in\Sigma^*} var_L(x) \leq \frac{m}{\delta^2}$.

Proof. The proof is almost identical to the one given over (Σ, E) in [5]. See Appendix A. $\square$

Proposition 6. *Let* $A := \langle \Sigma\cup\{\#\}, (O_c^A)_{c\in\Sigma}, \pi^A, F^A\rangle$ *and* $B := \langle \Sigma\cup\{\#\}, (O_c^B)_{c\in\Sigma}, \pi^B, F^B\rangle$ *be two* MON-1QFA*s Let* $\alpha, \beta \in \mathbb{R}$ *be non-negative real numbers such that* $\alpha+\beta =$

1. *We define the convex linear combination* $A \oplus B$ *of* A *and* B *w.r.t.* α *and* β *as follows,*

$$A \oplus B := \left\langle \Sigma \cup \{\#\}, (O_c^A)_{c\in\Sigma\cup\{\#\}} \oplus (O_c^B)_{c\in\Sigma\cup\{\#\}}, (\sqrt{\alpha}\cdot\pi^A) \oplus (\sqrt{\beta}\cdot\pi^B), F^A \cup F^B \right\rangle$$

Then $p_{A\oplus B}(x) = \alpha \cdot p_A(x) + \beta \cdot p_B(x)$ *holds for every* $x \in \Sigma^*$.

Proof. Let $x := x_1 \cdots x_n \in \Sigma^*$, then

$$p_{A\oplus B}(x) = \mathrm{Tr}\left(\sum_{r_j \in F_A \cup F_B} (P^A_{r_j}(\#) \oplus P^B_{r_j}(\#))\sigma_{A\oplus B}(x)(P^A_{r_j}(\#) \oplus P^B_{r_j}(\#)) \right)$$

Applying induction on n and basic properties of the $\dagger$ and $\oplus$ operators, we see what follows.

$$\sigma_{A\oplus B}(x_1\cdots x_n) = \alpha\sigma_A(x_1\cdots x_n) \oplus \beta\sigma_B(x_1\cdots x_n)$$

As an aftermath, the following chain of equations conclude the proof.

$$\begin{array}{rcl} p_{A\oplus B}(x) & = & \mathrm{Tr}\left(\sum_{r_j\in F_A\cup F_B}(P^A_{r_j}(\#)\oplus P^B_{r_j}(\#))\sigma_{A\oplus B}(x)(P^A_{r_j}(\#)\oplus P^B_{r_j}(\#))\right) \\ & = & \mathrm{Tr}\left(\sum_{r_j\in F_A\cup F_B}(P^A_{r_j}(\#)\oplus P^B_{r_j}(\#))(\alpha\sigma_A(x)\oplus\beta\sigma_B(x))(P^A_{r_j}(\#)\oplus P^B_{r_j}(\#))\right) \\ & = & \mathrm{Tr}\left(\sum_{rj\in F_A\cup F_B}\alpha(P^A_{r_j}(\#)\sigma_A(x)P^A_{r_j}(\#))\oplus\beta(P^B_{r_j}(\#)\sigma_B(x)P^B_{r_j}(\#))\right) \\ & = & \alpha\mathrm{Tr}\left(\sum_{r_j\in F_A}(P^A_{r_j}(\#)\sigma_A(x)P^A_{r_j}(\#))\right)+\beta\mathrm{Tr}\left(\sum_{r_j\in F_B}(P^B_{r_j}(\#)\sigma_B(x)P^B_{r_j}(\#))\right) \\ & = & \alpha p_A(x)+\beta p_B(x) \end{array}$$

$\square$

Lemma 3. *Let* A *be a* MON-1QFA *over* Σ^* *and let* L_A *be the language recognized by* A *with cut-point* $\lambda_A \neq 1/2$ *isolated by* $\delta > 0$. *Then there exists a* MON-1QFA A' *over* Σ *recognizing* $L'_A = L_A$ *with cut-point* $\lambda_{A'} = 1/2$ *isolated by* $\frac{\delta}{2\cdot max\{\lambda,1-\lambda\}}$.

Proof. Let denote by $\mathbf{1}$ the MON-1QFA with one pure-state only such that $p_{\mathbf{1}}(w) = 1$, for every $w \in \Sigma^*$. We have two cases: $0 < \lambda < 1/2$ and $1/2 < \lambda < 1$.

1. Assume $0 < \lambda < 1/2$. Then $1-2\lambda > 0$. Then the real numbers $\alpha := \frac{1}{2(1-\lambda)}$ and $\beta := \frac{1-2\lambda}{2(1-\lambda)}$ are non-negative and $\alpha+\beta = 1$. By Proposition 6 we can consider the following MON-1QFA over Σ,

$$A' := \left(\frac{1}{2(1-\lambda)}\cdot A\right) \oplus \left(\frac{1-2\lambda}{2(1-\lambda)}\cdot \mathbf{1}\right)$$

Observe that if $w \in L_A$ then $p_A(w) > \lambda + \delta$, hence

$$\begin{array}{rcl} p_{A'}(w) & = & \frac{1}{2(1-\lambda)}\cdot p_A(w) + \frac{1-2\lambda}{2(1-\lambda)}\cdot p_{\mathbf{1}}(w) \\ & > & \frac{1}{2(1-\lambda)}(\lambda+\delta) + \frac{1-2\lambda}{2(1-\lambda)}\cdot 1 \\ & = & \frac{1}{2} + \frac{\delta}{2(1-\lambda)} \end{array}$$

Otherwise $w \notin L_A$ imply $p_A(w) < \lambda - \delta$, thus

$$\begin{array}{rcc} p_{A'}(w) & = & \frac{1}{2(1-\lambda)} \cdot p_A(w) + \frac{1-2\lambda}{2(1-\lambda)} \cdot p_{\mathbf{1}}(w) \\ & < & \frac{1}{2(1-\lambda)}(\lambda - \delta) + \frac{1-2\lambda}{2(1-\lambda)} \cdot 1 \\ & = & \frac{1}{2} - \frac{\delta}{2(1-\lambda)} \end{array}$$

We conclude that A' recognizes L_A with cut-point $\lambda' := 1/2$ isolated by $\delta' := \frac{\delta}{2(1-\lambda)}$

2. Assume $1/2 < \lambda < 1$. Let denote by A^c the complement automaton of A. Then $p_{A^c}(w) = 1 - p_A(w)$ and $L_{A^c} = \Sigma^* \setminus L_A$ is recognized with cut-point $0 < \lambda_{A^c} = 1 - \lambda < 1/2$ isolated by $\delta_{A^c} = \delta$. Then, by the preceding case, we obtain an automaton $(A^c)'$ recognizing $\Sigma^* \setminus L_A$ with cut-point $\lambda_{(A^c)'} = 1/2$ isolated by $\delta_{(A^c)'} = \frac{\delta}{2(1-\lambda_{A^c})} = \frac{\delta}{2 \cdot \lambda}$. Consider the complement automaton of $(A^c)'$. We get another automaton A' recognizing L_A with cut-point $\lambda_{A'} = 1/2$ isolated by $\delta_{A'} = \frac{\delta}{2 \cdot \lambda}$.

□

To conclude this section, we link the family on MOn-1qfas with another class of quantum finite-state automata, known as the Latvian model of quantum finite state automata; it has been introduced by Ambainis, et.al in [1]. We will show that the MOn-1qfa model is in fact a subclass of the Latvian model.

Definition 10 (Latvian Automata). *A Latvian Automaton (*LQFA*) with m elementary pure states is a 5-tuple of the following form*

$$\langle \Sigma \cup \{\sharp\}, \{U_c\}_{c \in \Sigma \cup \{\sharp\}}, \{O_c\}_{c \in \Sigma \cup \{\sharp\}}, \pi_0, F \rangle$$

such that every $U_c \in \mathbb{C}^{m \times m}$ is a unitary matrix, i.e. $U_c^{-1} = U_c^{\dagger}$, and every $O_c \in \mathbb{C}^{m \times m}$ is a quantum observable, i.e. an Hermitian matrix. For each O_c we denote the set of its orthogonal eigenspaces by $\{E_1, \ldots, E_k\}$. For each E_i we denote by P_i the corresponding orthogonal projection matrix. The initial state of the system is denoted by $\pi_0 \in \mathbb{C}^{1 \times m}$. A Lavtian automaton recognizes languages by bounded (double-sided) error mode of acceptance. More precisely, we say that the automaton A recognizes the language L with bounded (two-sided) error if M accepts any $w \in L$ and rejects any $w \notin L$ with probability at least p where $p > \frac{1}{2}$. Observe that bounded (two-sided) error mode of acceptance is equivalent to δ-isolated λ cut-point mode of acceptance, provided that $\lambda = \frac{1}{2}$.

In [1] it is proved, as a main result, the following characterization in terms of block-group syntactic monoids.

Definition 11 (block-group monoids). *Let M be a finite monoid and let L, R denote respectively the left and the right Green's equivalence relations. If (and only if) every R-class and every L-class of M contains at most one idempotent element, then we say that M is a block-group. The class of block-group monoids is a pseudovariety of monoids, we denote it by* **BG**.

Theorem 4 (Ambainis et.al., [1])**.** *Let $L \in \Sigma^*$ be a formal language over the alphabet Σ. Then L is recognized by some* LQFA *if only if its syntactic monoid is a block-group.*

The following proposition shows that every MON-1QFA over Σ is in fact a LQFA with identical unitary evolutions.

Proposition 7. *The class of* MON-1QFA *over Σ is a sub-class of* LQFA*. In particular, let A be a* MON-1QFA *on Σ and let L_A be a language recognized by A with cut-point λ isolated by δ. Then there exists a* LQFA *A' recognizing $L_{A'} = L_A$ with bounded (two-sided) error $p = \frac{1}{2} + \frac{\delta}{2max\{\lambda,1-\lambda\}}$; that is to say with cut-point $\lambda' = \frac{1}{2}$ isolated by $\delta' = \frac{\delta}{2\cdot max\{\lambda,1-\lambda\}}$.*

Proof. Let A be a MON-1QFA over Σ recognizing L_A with cut-point λ isolated by $\delta > 0$. By Proposition 3, there exists a MON-1QFA over Σ, denoted by $A' = \langle \Sigma \cup \{\sharp\}, (O'_c)_{c\in\Sigma\cup\{\sharp\}}, \pi'_0, F'\rangle$, recognizing $L_{A'} = L_A$ with cut-point $\frac{1}{2}$ isolated by $\frac{\delta}{2\cdot\max\{\lambda,1-\lambda\}}$. Consider the Latvian automaton $B := \langle \Sigma \cup \{\sharp\}, (U_c), O'_c, F'\rangle$ defined by taking $U_c = I$ for every $c \in \Sigma$, where I is the identity matrix. Then $L_B = L'_A = L_A$ is recognized by B with bounded (two-sided) error given by $\frac{1}{2} + \frac{\delta}{2\cdot\max\{\lambda,1-\lambda\}}$. □

4 The syntactic monoids of LMO(Σ) languages

In this section we study the syntactic monoids of **LMO** languages. Observe that by Theorem 4 and by Proposition 7, if $L \in \mathbf{LMO}(\Sigma)$ then its syntactic monoid is a block-group. That is to say that $\mathbf{LMO}(\Sigma) \subseteq V_\Sigma(\mathbf{BG})$, as a sub boolean algebra.

In the next proposition we characterize the finite variation property in terms of properties satisfied by syntactic monoids of finite variation languages. By directly proving closure properties, it is not difficult to show that the class of finite variation regular languages is a $*$-variety of Eilenberg. In fact the following proposition holds true.

Proposition 8. *Let L be a regular language. The following propositions are equivalent.*

(i) L has finite variation.

(ii) Every strongly connected component of the minimum automaton recognizing L has one vertex only.

(iii) There exists a total ordering on the set Q of the states of the minimum automaton recognizing L such that $qa \geq q$ for every $q \in Q$ and every $a \in \Sigma$.

(iv) The syntactic monoid M of L is an R-trivial monoid.

Proof. (i) $\iff$ (ii) Consider the minimum automaton recognizing L and assume it admits a strongly connected component with more than one vertex, then there exists an oriented simple cycle p visiting at least two vertices. If $w \in \Sigma^*$ is the label word of p, then $\{w^n\}_{n\geq 1}$ shows that the variation is not finite. Vice-versa, assume that every strongly connected component is trivial. Then the variation is upper-bounded by the longest path with no self-loops and is therefore finite.
(ii) $\Rightarrow$ (iii) If we remove every self-loop from a graph we obtain an acyclic oriented graph. Consider the graph induced by the minimum automaton recognizing L and order the nodes of this graph by the topological ordering relation, then (iii) holds.
(iii) $\Rightarrow$ (iv) By hypothesis $qf \geq q$ for every $f \in \Sigma^*$ and $q \in Q$. Let M be the syntactic monoid of L. Assume that u and v generate the same right ideal of M, that is to say $uM = vM$. Then $u = vx$ and $v = uy$ for some $x, y \in \Sigma^*$. Hence for every q it holds $qu = qvx \geq qv = quy \geq qu$. That is $qu = qv$. It follows that $u = v$.
(iv) $\Rightarrow$ (ii) Assume that q and q' are in the same strongly connected component. Then, there exist two elements $u, v \in M$ such that $qu = q'$ and $q'v = q$. This imply $q(uv)^n = q$ and $q(uv)^n u = q'$ for every $n \in \mathbb{N}$. Pick an integer n such that $(uv)^n$ is idempotent. Then $(uv)^n$ generate the same right ideal of $(uv)^n u$, since $(uv)^n \in ((uv)^n u)M$. This imply that $(uv)^n = (uv)^n u$, since M is R-trivial by hypothesis. From this, it follows $q = q'$. □

Corollary 1. *Let L be a regular language. Then L has finite variation if and only if its syntactic monoid is $\mathbf{R}$-trivial.*

As a direct consequence, we have proved the following.

Proposition 9. *Let $L \in \boldsymbol{LMO}(\Sigma)$ be a language recognized by some* MON-1QFA *with isolated cutpoint. Then its syntactic monoid $M(L)$ is an R-trivial block-group. Formally $M(L) \in \mathbf{BG} \cap \mathbf{R}$ and $\boldsymbol{LMO}(\Sigma) \subseteq V_\Sigma(\mathbf{BG} \cap \mathbf{R})$ as a sub boolean algebra.*

Observe that the following holds true.

Proposition 10. *Every R-trivial block-group monoid is J-trivial.*

Proof. If S is a semigroup and $a \in S$, we say that a is regular if there exists $a \in S$ such that $asa = a$. We say that an L, R, J class is regular if all its elements are regular. If M is an R-trivial monoid then every regular J-class is a regular L-class C, such that every element of C is idempotent. The block group condition imply that C has at most one idempotent. Then C has only one element. Then every regular J-class of M is trivial and this imply that every J-class of M is trivial (see [20], pag. 65, Proposition 4.1). That is to say that M is a J-trivial monoid. □

By proposition 10, we have also proved the following.

Proposition 11. *Let $L \in \boldsymbol{LMO}(\Sigma)$ be a language recognized by some* MON-1QFA *with isolated cutpoint. Then its syntactic monoid $M(L)$ is J-trivial. Formally $M(L) \in \mathbf{J}$ and $\boldsymbol{LMO}(\Sigma) \subseteq V_\Sigma(\mathbf{J})$ as a sub boolean algebra.*

To conclude, we summarize the contents of this section in the following statement.

Proposition 12. *Let $L \in \boldsymbol{LMO}(\Sigma)$ be a language recognized by some* MON-1QFA *with isolated cutpoint. Then the following propositions holds.*

(i) *L is a picewise testable language, $L \in \boldsymbol{PT}$ or equivalently $L \in V_\Sigma(\mathbf{J})$.*

(ii) *L is literally idempotent $L \in liId$. Thus $L \in \boldsymbol{PT} \cap liId = V_\Sigma(\mathbf{J}) \cap liId$.*

(iii) *The syntactic monoid of L is J-trivial and literally satisfies the pseudoidentity $x^2 = x$. That is to say $L \in V_\Sigma(\overline{\mathbf{J}})$.*

(iv) *L lies in liId$\boldsymbol{PT}$, that is the boolean closure of languages of the following form, for any $k \geq 0$,*

$$\Sigma^* a_1 \Sigma^* a_2 \Sigma^* \cdots \Sigma^* a_k \Sigma^*, \text{ for } a_1, a_2, \ldots, a_k \in \Sigma \text{ and } a_i \neq a_{i+1} \text{ for every } 1 \leq i < k$$

Proof. (i) is exactly Proposition 10. (ii) follows from propositon 10 and the fact that projection operators P_i of any MON-1QFA 's observable are orthogonal and idempotent by definition. (iii) and (iv) follows from Theorem 3, due to Klíma and Polák. □

5 MOn-1qfas recognizing literally idempotent piecewise testable languages

We now show how languages in liId**PT** can be recognized by MON-1QFAs.

In this section it is convenient to define the language $L[a_1, \ldots, a_k] := \Sigma^* a_1 \Sigma^* \cdots \Sigma^* a_k \Sigma^*$, for any $k \geq 1$ and $a_1, \ldots, a_k \in \Sigma$, such that $a_i \neq a_{i+1}$ for each $1 \leq i < k$. We also let $S := \{a_1, \ldots, a_k\}$.

Definition 12 (On $j_i^{(\alpha)}$ indexes)**.** *Let $L[a_1, \ldots, a_k] := \Sigma^* a_1 \Sigma^* \cdots \Sigma^* a_k \Sigma^*$, for any $k \geq 1$ and $a_1, \ldots, a_k \in \Sigma$, such that $a_i \neq a_{i+1}$ for each $1 \leq i < k$. Let $S := \{a_1, \ldots, a_k\}$. For every $\alpha \in S$, let $\#\alpha$ be the number of times that α appears as a letter in the word $a_1 a_2 \cdots a_k$. Let*

$$j_1^{(\alpha)} < j_2^{(\alpha)} < \cdots < j_{\#\alpha}^{(\alpha)} \text{ be all the indexes such that } \alpha = a_{j_1^{(\alpha)}} = \ldots = a_{j_{\#\alpha}^{(\alpha)}}$$

in increasing order. For each $1 \leq i \leq \#\alpha$ it holds that $1 \leq j_i^{(\alpha)} \leq k$.

Definition 13. *We define, for every $\alpha \in S$, two orthogonal projectors of dimension $(k+1)\times(k+1)$: the up operator $P^{(k)}_{\nearrow}(\alpha)$ and the down operator $P^{(k)}_{\searrow}(\alpha)$, such that*

$$\left(P^{(k)}_{\nearrow}(\alpha)\right)_{rs} = \begin{cases} 1 & \text{if } r = s \text{ and } \forall\, 1 \le i \le \#\alpha \text{ it holds } r, s \notin \{j_i^{(\alpha)}, j_i^{(\alpha)}+1\}, \\ \frac{1}{2} & \text{if } \exists\, 1 \le i \le \#\alpha \text{ such that } r, s \in \{j_i^{(\alpha)}, j_i^{(\alpha)}+1\}, \\ 0 & \text{otherwise,} \end{cases}$$

$$\left(P^{(k)}_{\searrow}(\alpha)\right)_{rs} = \begin{cases} \frac{1}{2} & \text{if } r = s \text{ and } \exists\, 1 \le i \le \#\alpha \text{ such that } r, s \in \{j_i^{(\alpha)}, j_i^{(\alpha)}+1\}, \\ -\frac{1}{2} & \text{if } r \neq s \text{ and } \exists\, 1 \le i \le \#\alpha \text{ such that } r, s \in \{j_i^{(\alpha)}, j_i^{(\alpha)}+1\}, \\ 0 & \text{otherwise.} \end{cases}$$

Definition 14. *We also give an extended representation of $P^{(k)}_{\nearrow}$ and $P^{(k)}_{\searrow}$. To begin, consider the following two elementary operators of orthogonal projection in dimension 2×2, the up-diagonal operator $P_{\nearrow}$ and the down-diagonal operator $P_{\searrow}$, defined as*

$$P_{\nearrow} := \begin{bmatrix} +\frac{1}{2} & +\frac{1}{2} \\ +\frac{1}{2} & +\frac{1}{2} \end{bmatrix} \qquad P_{\searrow} := \begin{bmatrix} +\frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & +\frac{1}{2} \end{bmatrix}$$

Then, for $k > 1$, the up-diagonal operator $P^{(k)}_{\nearrow}(\alpha) \in \mathbb{C}^{(k+1)\times(k+1)}$ is defined as follows

	$1,\dots$	$j_1^{(\alpha)}$ $j_1^{(\alpha)}+1$		$j_2^{(\alpha)}$ $j_2^{(\alpha)}+1$		$\cdots$		$j_{\#\alpha}^{(\alpha)}$ $j_{\#\alpha}^{(\alpha)}+1$	$\dots, k+1$
$1,\dots$	I								
$j_1^{(\alpha)}$ $j_1^{(\alpha)}+1$		$P_{\nearrow}$							
			I						
$j_2^{(\alpha)}$ $j_2^{(\alpha)}+1$				$P_{\nearrow}$					
					I				
$\vdots$						$\ddots$			
							I		
$j_{\#\alpha}^{(\alpha)}$ $j_{\#\alpha+1}^{(\alpha)}$								$P_{\nearrow}$	
$\dots, k+1$									I

in which not appearing elements are intended to be null, and every I is an identity matrix.

Next, for $k > 1$, we define $P^{(k)}_{\searrow}(\alpha) \in \mathbb{C}^{(k+1)\times(k+1)}$ as follows

	$1,\ldots$	$j_1^{(\alpha)}\quad j_1^{(\alpha)}+1$		$j_2^{(\alpha)}\quad j_2^{(\alpha)}+1$		$\cdots$		$j_{\#\alpha}^{(\alpha)}\quad j_{\#\alpha+1}^{(\alpha)}$	$\ldots,k+1$	
$1,\ldots$	$\mathbf{0}$									
$j_1^{(\alpha)}$ $j_1^{(\alpha)}+1$		$P_{\searrow}$								
			$\mathbf{0}$							
$j_2^{(\alpha)}$ $j_2^{(\alpha)}+1$				$P_{\searrow}$						
					$\mathbf{0}$					
$\vdots$						$\ddots$				
							$\mathbf{0}$			
$j_{\#\alpha}^{(\alpha)}$ $j_{\#\alpha+1}^{(\alpha)}$								$P_{\searrow}$		
$\ldots,k+1$									$\mathbf{0}$	

in which not appearing elements are intended to be null and the **0** *entries are block matrices with null elements.*

Proposition 13. *Definition 13 and Definition 14 are equivalent.*

Definition 15. *Let $S := \{a_1, \ldots, a_k\}$ for some $a_i \in \Sigma$. By calling e_j the boolean row vector such that $(e_j)_i = 1 \Leftrightarrow i = j$, we define $A[a_1, \ldots, a_k] = \langle \Sigma \cup \{\#\}, \pi_0^{(k)}, \{O_c^{(k)}\}_{c \in \Sigma \cup \{\#\}}, F^{(k)} \rangle$ as the* MON-1QFA *where*

- *$\pi_0^{(k)} = e_1 \in \mathbb{C}^{1\times(k+1)}$,*
- *for $\alpha \in S$, the associated projectors of $O_\alpha^{(k)}$ are $P^{(k)}_{\nearrow}(\alpha)$ and $P^{(k)}_{\searrow}(\alpha)$,*
- *with each $O_c^{(k)}$ such that $c \in \Sigma \setminus S$, we associate the identity matrix $I_{(k+1)\times(k+1)}$,*
- *the projector of the accepting result of $O_\#^{(k)}$ is $(e_{k+1})^T e_{k+1}$, i.e. the $(k+1)\times(k+1)$ boolean matrix having a 1 only in the bottom right entry. We denote it by P_{acc}.*

We begin a careful analysis of the computing behavior of $A[a_1, \ldots, a_k]$ as defined in Definition 15. We begin with some lemmata.

Lemma 4. *Consider the* MON-1QFA *$A[a_1, \ldots, a_k]$ with up-diagonal projectors $\{P^{(k)}_{\nearrow}(\alpha)\}_{\alpha \in S}$, for $S := \{a_1, \ldots, a_k\}$. Let $\mathbf{x} = (x_1, x_2, \ldots, x_{k+1}) \in \mathbb{R}^{1\times(k+1)}$ be an n-dimensional real vector. Let $j_1^{(\alpha)} < \cdots < j_{\sharp\alpha}^{(\alpha)}$ be the indexes as defined in*

Definition 12. Let $\mathbf{y} := \mathbf{x}P^{(k)}_{\nearrow}(\alpha)$. *Then*

$$(\mathbf{y})_i = \begin{cases} (\mathbf{y})_i & \text{if } i \notin \{j_1^{(\alpha)}, \ldots, j_{\#\alpha}^{(\alpha)}\} \cup \{j_1^{(\alpha)}+1, \ldots, j_{\#\alpha}^{(\alpha)}+1\} \\ \frac{(\mathbf{y})_i + (\mathbf{y})_{i+1}}{2} & \text{if } i \in \{j_1^{(\alpha)}, \ldots, j_{\#\alpha}^{(\alpha)}\} \\ \frac{(\mathbf{y})_{i-1} + (\mathbf{y})_i}{2} & \text{if } i \in \{j_1^{(\alpha)}+1, \ldots, j_{\#\alpha}^{(\alpha)}+1\} \end{cases}$$

Proof. We will show that $P^{(\alpha)}_{\nearrow}(\alpha)$ sends contiguous pairs of coordinates of $\mathbf{x}$ into their mid-points, according to the indexes $\{j_q^{(\alpha)}\}_{q=1}^{\#\alpha}$. If $i \notin \{j_1^{(\alpha)}, \ldots, j_{\#\alpha}^{(\alpha)}\} \cup \{j_1^{(\alpha)}+1, \ldots, j_{\#\alpha}^{(\alpha)}+1\}$ then $P^{(k)}_{\nearrow}(\alpha)$, by Definition 14, sends the i-th coordinate $(\mathbf{y})_i$ to itself. If $i \in \{j_1^{(\alpha)}, \ldots, j_{\#\alpha}^{(\alpha)}\}$ then $P^{(k)}_{\nearrow}(\alpha)$, by Definition, 14 sends the $i, (i+1)$-th coordinates $\big((\mathbf{y})_i, (\mathbf{y})_{i+1}\big)$ to $\big((\mathbf{y})_i, (\mathbf{y})_{i+1}\big) \cdot ((\frac{1}{2}, \frac{1}{2})^T(1,1)) = \big(\frac{(\mathbf{y})_i + (\mathbf{y})_{i+1}}{2}, \frac{(\mathbf{y})_i + (\mathbf{y})_{i+1}}{2}\big)$. If $i \in \{j_1^{(\alpha)}+1, \ldots, j_{\#\alpha}^{(\alpha)}+1\}$ then $P^{(k)}_{\nearrow}(\alpha)$, by Definition, 14 sends the $(i-1), i$-th coordinates $\big((\mathbf{y})_{i-1}, (\mathbf{y})_i\big)$ to $\big((\mathbf{y})_{i-1}, (\mathbf{y})_i\big) \cdot ((\frac{1}{2}, \frac{1}{2})^T(1,1)) = \big(\frac{(\mathbf{y})_{i-1} + (\mathbf{y})_i}{2}, \frac{(\mathbf{y})_{i-1} + (\mathbf{y})_i}{2}\big)$. This concludes the proof. $\square$

Lemma 5. *Consider the language* $L[a_1, \ldots, a_k]$ *over the alphabet* Σ *and let* $S := \{a_1, \ldots, a_k\}$. *Let* $w := w_1 \cdots w_n$ *be a word of* Σ^*. *Consider the class of up-diagonal orthogonal projectors* $\{P^{(k)}_{\nearrow}(a_i)\}_i$ *associated to the* MON-1QFA $A[a_1, \ldots, a_k]$, *with initial quantum state* $\pi_0 := e_1 \in \mathbb{C}^{1 \times (k+1)}$. *Let us define*

$$\pi := \pi_0 P^{(k)}_{\nearrow}(w_1) P^{(k)}_{\nearrow}(w_2) \cdots P^{(k)}_{\nearrow}(w_n)$$

where, for notational convenience, $P^{(k)}_{\nearrow}(w_i) = I$ *if* $w_i \in \Sigma \backslash S$. *Then the following two propositions holds:*

1. *if* $w \in L[a_1, \ldots, a_k]$ *then, for every* $1 \leq i \leq k+1$, $(\pi)_i > 0$.
2. *for every* $1 \leq j \leq i \leq k+1$, *it holds that:*

$$\text{if } (\pi)_i > 0 \text{ then } (\pi)_j \geq 2^{-k}$$

Proof. Observe that by Lemma 4 any projector $P^{(k)}_{\nearrow}(\alpha)$ sends contiguous pairs of coordinates into their mid-point according to indexes $\{j_q^{(\alpha)}\}_{q=1}^{\#\alpha}$ and leaves the others coordinates intact.
We prove (i). If $w \in L[a_1, \ldots, a_k]$ then $w = u_1 a_1 u_2 a_2 \cdots u_k a_k u_{k+1}$ for some $u_1, \ldots, u_{k+1} \in \Sigma^*$. As we start with e_1, by applying a projector $P^{(k)}_{\nearrow}(\alpha)$ to e_1 as defined in Definition 14, we perturb the second coordinate from a null to a non null value if and only if $j_1^{(\alpha)} = 1$, that is if and only if $\alpha = a_1$; otherwise we leave e_1 intact. Once we have applied $P^{(k)}_{\nearrow}(a_1)$, we perturb the third coordinate of the vector state if and only if $j_1^{(\alpha)} = 2$, that is if and only if $\alpha = a_2$; otherwise, by applying any other up-diagonal projector we leave perturbed coordinates with a non null value. Iterating this way, once we have applied $P^{(k)}_{\nearrow}(a_i)$ we have perturbed the $i+1$-th coordinate, and we perturb the $i+2$-th coordinate if and

only if we apply $P^{(k)}_{\nearrow}(a_{i+1})$, leaving the previously perturbed coordinates with a non null value otherwise. The thesis follows.
Now we prove (ii). For any $k \in \mathbb{N}_0$, any $\mathbf{x} \in \mathbb{R}^{1\times(k+1)}$ and each $1 \le i \le k$ let $T_i : \mathbb{R}^{1\times(k+1)} \to \mathbb{R}^{1\times(k+1)}$ be the linear transformation defined by

$$(T_i(\mathbf{x}))_j := \begin{cases} (\mathbf{x})_j & \text{if } j \notin \{i, i+1\} \\ \frac{(\mathbf{x})_j + (\mathbf{x})_{j+1}}{2} & \text{if } j = i \\ \frac{(\mathbf{x})_{j-1} + (\mathbf{x})_j}{2} & \text{if } j = i+1 \end{cases}$$

In order to prove our thesis it is sufficient to prove the following equivalent statement. For any length $n \in \mathbb{N}_0$, any choice of indexes $1 \le i_1, \ldots, i_n \le k$ and any $1 \le j \le i \le k+1$, it holds, provided we defined $T_{[n]}(e_1) := T_{i_n} \circ \cdots \circ T_{i_1}(e_1)$, that

$$\text{if } \left(T_{[n]}(e_1)\right)_i > 0 \text{ then } \left(T_{[n]}(e_1)\right)_j \ge 2^{-k}$$

We proceed by induction on $k \in \mathbb{N}_0$. Let $k = 1$, then $T_{[n]}(e_1) = (1/2, 1/2)$ for every $n \in \mathbb{N}_0$ and the thesis follows. Now let $k > 1$ and analyze the inductive step for $k+1$. Let $1 \le m \le n$ be the greatest integer such that the transformed $(k+1)$-th coordinate satisfies $\left(T_{[m]}(e_1)\right)_{k+1} = 0$. Then we do not loose generality by reasoning in dimension k instead of $k+1$, since by applying T we are just replacing contiguous coordinate pairs by their mid-points and we start from e_1. Hence, induction hypothesis applies. As a consequence, it holds that for every $1 \le j \le i \le k+1$,

$$\text{if } (T_{[m]}(e_1))_i > 0 \text{ then } (T_{[m]}(e_1))_j \ge 2^{-(k-1)}$$

If $m = n$, we are done. Otherwise it must hold that

$$\left(T_{[m+1]}(e_1)\right)_{k+1} = \frac{\left(T_{[m]}(e_1)\right)_k}{2} \ge 2^{-k}$$

Thus, for every $1 \le i \le k+1$ we have $\left(T_{[m+1]}(e_1)\right)_i \ge 2^{-k}$. Subsequent applications of T can not decrease this bound, since T replace contiguous coordinates pairs by their mid-point. This imply the thesis. $\square$

Lemma 6. *Fix a positive integer $i \in \mathbb{N}_0$. For any $k > i$ and any $S := \{a_1, \ldots, a_k\}$ consider the* MON-1QFA *$A := A[a_1, \ldots, a_k]$ and its associated projectors. Let $w \in L[a_1, \ldots, a_i] \setminus L[a_1, \ldots, a_{i+1}]$ be of length $|w| = n$. Then for every $d_1, d_2, \ldots, d_n \in \{\nearrow, \searrow\}$ and for every $m \in \mathbb{N}_0$ such that $i+2 \le m \le k+1$ it holds that*

$$\left(\pi_0 P^{(k)}_{d_1}(w_1) \cdots P^{(k)}_{d_n}(w_n)\right)_m = 0$$

Where, for notational convenience, $P^{(k)}(c)_{\searrow} = P^{(k)}(c)_{\nearrow} = I$ if $c \in \Sigma \setminus S$ and I is the identity matrix of size $(k+1) \times (k+1)$.

Proof. For every $x \in \Sigma^*$ of length $|x|$ and every $\mathbf{d} = (d_1, \ldots, d_{|x|}) \in \{\searrow, \nearrow\}^{|x|}$, we shall denote $P_{\mathbf{d}}(x) := P^{(k)}_{d_1}(x_1) \cdots P^{(k)}_{d_{|x|}}(x_{|x|})$. We proceed by induction on

$i \in \mathbb{N}_0$. If $i = 1$, then $w \in L[a_1] \setminus L[a_1, a_2]$ imply that $w = w' a_1 w''$ such that w' does not contains the letter a_1 and w'' does not contains the letter a_2. Then, because of Definition 14, for every $\mathbf{d}$, it holds that

$$\text{if } q \geq 2 \text{ then } (\pi_0 P_{\mathbf{d}}(w'))_q = 0$$

since the projectors $P_{\nearrow}(a_1), P_{\searrow}(a_1)$ of a_1 are never applied and they are the only projectors of A which can perturb the second coordinate from a null to a non non-null value.
Then for every $\mathbf{d}$ and $d \in \{\searrow, \nearrow\}$ it holds that

$$\text{if } q \geq 3 \text{ then } \left(\pi_0 P_{\mathbf{d}}(w') P_d(a_1)\right)_q = 0$$

since the projector $P_d(a_1)$ disrupt, at most, the second coordinate $(\pi_0 P_{\mathbf{d}}(w') P_d(a_1))_2$.
Since w'' does not contains the letter a_2, then for every $\mathbf{d}', \mathbf{d}''$ it holds that

$$\text{if } q \geq 3 \text{ then } \left(\pi_0 P_{\mathbf{d}}(w') P_{d'}(a_1) P_{\mathbf{d}''}(w'')\right)_q = 0$$

because the projectors $P_{\nearrow}(a_2), P_{\searrow}(a_2)$ are never applied. This proves the base case of induction.

Let us suppose that the thesis is true for i, we analyze $i+1$. Then $w \in L[a_1, \ldots, a_{i+1}] \setminus L[a_1, \ldots, a_{i+2}]$ so there exist words w', w'' such that $w = w' a_{i+1} w''$ where $w' \in L[a_1, \ldots, a_i] \setminus L[a_1, \ldots, a_{i+1}]$ and w'' does not contains a_{i+2}. By induction hypothesis, for every $\mathbf{d}$ and $k > i$ it holds that

$$\text{if } i+2 \leq q \leq k+1 \text{ then } \left(\pi_0 P^{(k)}_{\mathbf{d}}(w')\right)_q = 0$$

Then for every $\mathbf{d}$ and $d \in \{\searrow, \nearrow\}$ it holds that

$$\text{if } i+3 \leq q \leq k+1 \text{ then } \left(\pi_0 P^{(k)}_{\mathbf{d}}(w') P^{(k)}_d(a_{i+1})\right)_q = 0$$

since the projector $P^{(k)}_d(a_{i+1})$ disrupt, at most, the i+2 coordinate $(\pi_0 P^{(k)}_{\mathbf{d}}(w') P^{(k)}_d(a_{i+1}))_{i+2}$.
Since w'' does not contains the letter a_2, then for every $\mathbf{d}', \mathbf{d}''$ it holds that

$$\text{if } i+3 \leq q \leq k+1 \text{ then } \left(\pi_0 P^{(k)}_{\mathbf{d}'}(w') P^{(k)}_d(a_{i+1}) P^{(k)}_{\mathbf{d}''}(w'')\right)_q = 0$$

This concludes the proof. □

Finally, we are ready to characterize $L[a_1, \ldots, a_k]$ recognition with isolated cut-point by $A[a_1, \ldots, a_k]$ automata.

Theorem 5. *The automaton $A[a_1, \ldots, a_k]$ recognizes $L[a_1, \ldots, a_k]$ with cutpoint $\lambda = \frac{1}{2^{2k+1}}$ isolated by $\delta = \frac{1}{2^{2(k+1)}}$.*

Proof. We seek a lower-bound for $p_A(t)$, for $t \in \Sigma^*$. According to Proposition 1 we have

$$p_A(t) = \sum_{r_j \in F} \sum_{j_1,\ldots,j_n} ||\pi_0 P_{j_1}(t_1)\cdots P_{j_n}(t_n)P_{r_j}(\#)||_2^2$$

From Lemma 5, item (i), it follows that

$$\text{if } t \in L[a_1,\ldots,a_k] \text{ then } \left(\pi_0 P^{(k)}_{\nearrow}(t_1)\cdots P^{(k)}_{\nearrow}(t_n)\right)_{k+1} > 0$$

As an aftermath, the following chain of equations and inequalities holds true:

$$\begin{array}{rcll}
p_A(t) & = & \sum_{r_j\in F}\sum_{j_1,\ldots,j_n} ||\pi_0 P_{j_1}(t_1)\cdots P_{j_n}(t_n)P_{r_j}(\#)||_2^2 & \\
& = & \sum_{j_1,\ldots,j_n\in\{\nearrow,\searrow\}} ||\pi_0 P_{j_1}(t_1)\cdots P_{j_n}(t_n)P_{\mathrm{acc}}(\#)||_2^2 & \\
& = & \sum_{j_1,\ldots,j_n\in\{\nearrow,\searrow\}} ||\left(\pi_0 P_{j_1}(t_1)\cdots P_{j_n}(t_n)\right)_{k+1}||_2^2 & \\
& \geq & ||\pi_0 P_{\nearrow}(t_1)\cdots P_{\nearrow}(t_n)P_{\mathrm{acc}}(\#)||_2^2 & ||\cdot||_2^2 \geq 0 \\
& = & \left(\left(\pi_0 P_{\nearrow}(t_1)\cdots P_{\nearrow}(t_n)\right)_{k+1}\right)^2 & \text{by definition of } P_{\mathrm{acc}}(\#) \\
& \geq & 2^{-2k} & \text{Lemma 5}
\end{array}$$

From Lemma 6 we have the following implication:

$$\text{if } t \notin L[a_1,\ldots,a_k] \text{ then } \sum_{j_1,\ldots,j_n\in\{\nearrow,\searrow\}} ||\left(\pi_0 P_{j_1}(t_1)\cdots P_{j_n}(t_n)\right)_{k+1}||_2^2 = 0$$

hence

$$\text{if } t \notin L[a_1,\ldots,a_k] \text{ then } p_A(t) = 0$$

This concludes the proof. □

Since the class liId**PT** is the boolean closure of languages of the form $L[a_1,\ldots,a_k]$, and $\mathbf{LMO}(\Sigma)$ is a boolean algebra, Theorem 5 implies that all literally idempotent piecewise testable languages can be recognized by MOn-1qfas. We summarize our algebraic characterization result in the following statement.

Theorem 6 (Algebraic Characterization of $\mathbf{LMO}(\Sigma)$ languages)**.** *Let $L \in \Sigma^*$ be a formal language. Then the following four propositions are equivalent.*

(i) L is recognized with isolated cut-point by some MOn-1qfa.

(ii) the syntactic monoid of L is a J-trivial finite monoid and literally satisfies the idempotency pseudoidentity $x^2 = x$.

(iii) L is a literal idempotent and piecewise testable language.

(iv) L lies in the boolean closure of languages of the following form, for any $k \geq 0$,

$\Sigma^* a_1 \Sigma^* a_2 \Sigma^* \cdots \Sigma^* a_k \Sigma^*$, *for $a_1, a_2, \ldots, a_k \in \Sigma$ and $a_i \neq a_{i+1}$ for every $1 \leq i < k$*

6 Algorithmic and logical conclusions

Theorem 6 allows us to prove the existence of a polynomial time algorithm for deciding $\mathbf{LMO}(\Sigma)$ membership. In this way, we solve the polynomial-time decidability question for **LMO** in the affirmative direction.

Theorem 7. *Given a regular language $L \in \Sigma^*$, the problem of determining whether $L \in \boldsymbol{LMO}(\Sigma)$ is decidable in time $O((|Q|+|\Sigma|)^2)$, where $|Q|$ is the size of the minimal deterministic automaton for L.*

Proof. This algorithm first constructs the minimal deterministic automaton A_L for L in time $O(|Q|\log(|Q|))$ as shown in [14]. Then, in time $O(|Q|+|\Sigma|)$, it checks whether L is literally idempotent by visiting all the vertices and edges in the graph of A_L. Finally, it verifies whether L is piecewise testable in time $O((|Q|+|\Sigma|)^2)$ with the technique shown in [23]. The fact that $\mathbf{LMO}(\Sigma) = \text{liId}\mathbf{PT}(\Sigma)$ completes the proof. □

We conclude this last section with some remarks from mathematical logic. The piecewise testable languages are known in literature to be exactly those languages definable in the boolean closure of the existential first-order logic $\Sigma_1[<]$, denoted by $\text{Bool}(\Sigma_1[<])$ [21]. We would like to characterize it here the logical definability of **LMO** languages as well. With this in mind, we set a first-order syntax with atomic formulae of the following type:

$$\lambda(x) = a \text{ and } x < y \text{ and } \top$$

where x, y are variables, $a \in \Sigma$ is a letter and $\top$ is a constant which means *true*. If φ, ψ are first-order formulae, then

$$\neg\varphi \text{ and } \varphi \vee \psi \text{ and } \exists x \varphi$$

are first-order formulae as well. In order to introduce a semantics in terms of words of Σ^*, we let the variables range over positions of words. A variable not quantified is called a *free* variable, then a *sentence* is a formula without free variables. Let the free variables of the formula φ range in a subset of $\{x_1, \ldots, x_n\}$. Each x_i is associated with a position j_i of w. In this way, we can consider the truth value of φ and denote it by $w, j_1, \ldots, j_n \models \varphi$. To any first-order sentence φ we associate the language $L(\varphi) = \{w \in \Sigma^* | w \models \varphi\}$. We recall that the existential first order fragment $\Sigma_1[<]$ is given by first-order formulae in which we allow just one block of existential quantifiers and no blocks on universal quantifiers, in the prenex-normal form. Now let us consider the language $L[a_1, \ldots, a_k]$ given by

$$\Sigma^* a_1 \Sigma^* a_2 \Sigma^* \cdots \Sigma^* a_k \Sigma^*, \text{ for } a_1, a_2, \ldots, a_k \in \Sigma \text{ and } a_i \neq a_{i+1} \text{ for every } 1 \leq i < k$$

then we shall define the following $\Sigma_1[<]$ formulae, we call them the *easy* formulae of the existential first-order logic:

$$\varphi[a_1, \ldots, a_k] := \exists x_1 \cdots \exists x_k \left(\bigwedge_{i=1}^{k-1} x_i < x_{i+1} \wedge \bigwedge_{i=1}^{k} \lambda(x_i) = a_i \wedge \bigwedge_{i=1}^{k-1} \neg(\lambda(x_i) = a_{i+1}) \right)$$

Then clearly $\varphi[a_1, \ldots, a_k] \in \Sigma_1[<]$ and, by induction on k, it is possible to prove that $L(\varphi[a_1, \ldots, a_k]) = L[a_1, \ldots, a_k]$. This proves the following logical characterization of **LMO** :

Proposition 14. ***LMO*** *is exactly the class of languages definable by boolean combinations of* easy *formulae of the existential first-order logic* $\Sigma_1[<]$.

Also, we would like to take into account the *linear temporal logic without the next operator* (LTLWN). The syntax and semantics of LTLWN is the same as the already presented semantics for first-order formulae, but we also consider the *until* binary operator $\mathbb{U}$ whose semantics is defined as follows.

$$w \models \varphi_1 \mathbb{U} \varphi_2 \iff \exists i \in \mathbb{N} \text{ s.t. } w_i \models \varphi_2 \text{ and } \forall 1 \leq j < i : w_j \models \varphi_1$$

Let Σ be an alphabet and let $\Gamma_1, \ldots, \Gamma_k \subseteq \Sigma$ be non-empty sets. Define $\varphi_{\Gamma_i} := \bigvee_{b \in \Gamma_i} b$ and $\varphi_\epsilon = \neg\varphi_\Sigma$. As Klíma and Polák in [15], we shall consider the following formulae of LTLWN $\varphi[B_1, \ldots, B_k]$ and call them the *easy* formulae of LTLWN:

$$\varphi([\Gamma_1, \ldots, \Gamma_k]) := \varphi_{\Gamma_1} \mathbb{U}(\varphi_{\Gamma_2} \mathbb{U}(\cdots(\varphi_{\Gamma_n} \mathbb{U} \varphi_\epsilon)) \cdots)$$

It is possible to prove that $L(\varphi_{\Gamma_i}) = \Gamma_i \Sigma^*$ and that $\varphi_\epsilon = \epsilon$. Moreover that $L([\Gamma_1, \ldots, \Gamma_k]) = \Gamma_1^* \cdots \Gamma_k^*$. This imply that L is definable as a boolean combination of *easy* formulae of LTLWN if and only if it is a literally idempotent piecewise testable language, as proved in [15]. We get the following immediate corollary, which concludes our work on MON-1QFAs.

Proposition 15. ***LMO*** *is exactly the class of languages definable by boolean combinations of* easy *formulae of the linear temporal logic without the next operator LTLWN.*

References

[1] A. Ambainis, M. Beaudry, M. Golovkins, A. Kikusts, M. Mercer, D. Thérien, *Algebraic Results on Quantum Automata*, Theory Comp. Syst., vol. 39(1), (2006), 165-188.

[2] A. Bertoni, A. Brambilla, G. Mauri, N. Sabadini *An application of the theory of free partially commutative monoids: asymptotic densities of trace languages*, In: Proceedings of the 10th mathematical foundations of computer science. (1981) LNCS 118, Springer, pp 205-215.

[3] A. Bertoni, M. Carpentieri, *Regular Languages Accepted by Quantum Automata*, Inf. Comput., vol. 165(2), (2001), 174-182.

[4] A. Bertoni, C. Mereghetti, B. Palano, *Quantum Computing: 1-Way Quantum Automata* Developments in Language Theory 2003: 1-20

[5] A. Bertoni, C. Mereghetti, B. Palano, *Trace monoids with idempotent generators and measure-only quantum automata*, Natural Comp., vol. 9(2), (2010), 383-395.

[6] J. R. Büchi, *Weak second-order arithmetic and finite automata*. Zeitschrift für mathematische Logik und Grundlagen der Mathematik, 6:6692, 1960.

[7] A. Brodsky, N. Pippenger, *Characterizations of 1-Way Quantum Finite Automata*, SIAM J. Comput., vol. 31(5), (2002), 1456-1478.

[8] The book of traces. (1995) World Scientific, Singapore.

[9] S. Eilenberg, *Automata, languages, and machines*, vol. A, vol. B, Academic Press, 1976.

[10] Z. Esik and M. Ito, *Temporal logic with cyclic counting and the degree of aperiodicity in finite automata*, Acta Cybernetica 16 (2003), 1-28.

[11] Z. Esik and K.G. Larsen, *Regular languages defined by Linström quantifiers*, Theoretical Informatics and Applications 37 (2003), 197-242.

[12] D. Gottesman , I. Chuang (1999) *Quantum teleportation as a universal computational primitive*. Nature 402:390393. arXiv:quant-ph/9908010

[13] J. Gruska, *Quantum computing*, (1999), McGraw-Hill

[14] J.E. Hopcroft, *An N Log N Algorithm for Minimizing States in a Finite Automaton*, Technical Report. Stanford University, Stanford, CA, USA, 1971.

[15] O. Klíma, L. Polák, *On Varieties of Literally Idempotent Languages*, ITA 42(3), (2008), 583-598.

[16] M. Kunc, *Equational description of pseudovarieties oh homomorphisms*, Theoretical Informatics and Applications 37 (2003), 243-254

[17] A. Kondacs, J. Watrous, *On the Power of Quantum Finite State Automata*, FOCS (1997) 66-75.

[18] D. W. Leung (2004) Quantum computation by measurements. Int J Quant Inf 2:3343. arXiv:quant-ph/ 0310189, 2003

[19] Nielsen MA (2003) Quantum computation by measurement and quantum memory. Phys Lett A 308:96100. arXiv:quant-ph/0108020

[20] J. E. Pin, *Varieties of formal languages*, North Oxford, London and Plenum, New-York, 1986.

[21] I. Simon, *Piecewise testable events*, Automata Theory and Formal Languages, (1975), Springer, Lecture Notes in Computer Science, vol 33.

[22] H. Straubing, *On logical descriptions of regular languages*, Proc. Latin 2002, Springer Lecture Notes in Computer Science, Vol. 2286, 2002, 528-538.

[23] A.N. Trahtman, *Piecewise and Local Threshold Testability of DFA*, FCT (2001), 347-358.

A Appendix A

A.1 Proof of Proposition 2

The formal power series generated by a MON-1QFA A on Σ with m states admits a linear representation $\langle \xi, (P(c))_{c\in\Sigma}, \eta\rangle$ where $||\xi|| = 1$, $P(c)$ is a projector for all $c \in \Sigma$ and $||\eta|| \leq \sqrt{m}$.

Proof. Given a matrix $M \in \mathbb{C}^{m\times m}$ with rows $r_1, \dots, r_m$, let $\varphi(M)$ be the vector $(r_1, \dots, r_m) \in \mathbb{C}^{1\times m^2}$. Let A be a MON-1QFA over Σ with with π_0 as initial state, the observable O_c described by projectors $P_1(c), \dots, P_k(c)$ for any $c \in \Sigma$, the observable $O_\sharp$ described by projectors $P_1(\sharp), \dots, P_s(\sharp)$ and $F \subseteq \{r_1, \dots, r_s\}$. For any $w := w_1 \cdots w_n \in \Sigma^*$, Proposition 1 imply

$$p_A(w) = \mathrm{Tr}\left(\sum_{r_j\in F}\sum_{k_1,\dots,k_n} ||\pi_0 P_{k_1(w_1)\cdots P_{k_n}(w_n)P_j(\sharp)}||^2\right)$$

Consider the formal series $\psi : \Sigma^* \to \mathbb{C}$ whose linear representation is given by:

$$\left(\pi_0 \otimes \pi_0^*, \left(P(c) := \sum_j P_j(c) \otimes P_j(c)^*\right)_{c\in\Sigma}, \eta := \varphi(I) \cdot \sum_{r_k\in F} P_k(\sharp) \otimes P_k(\sharp)\right)$$

where I is the identity matrix. Then

$$\begin{array}{rcc}
\psi(w_1 \cdots w_n) & = & (\pi_0 \otimes \pi_0^*)(P(w_1)\dots P(w_n))(\varphi(I) \cdot \sum_{r_k\in F} P_k(\sharp) \otimes P_k(\sharp)^*)^T \\
& = & \sum_{r_k\in F, j_1,\dots,j_n} \Big[\pi_0 P_{j_1}(w_1) \cdots P_{j_n}(w_n) P_{r_k}(\sharp) \otimes \\
& & \pi_0^* P_{j_1}(w_1)^* \cdots P_{j_n}(w_n)^* P_{r_k}(\sharp)^*\Big]\varphi(I)^T \\
& = & \sum_{r_k\in F, j_1,\dots,j_n} \sum_j (\pi_0 P_{j_1}(w_1) \cdots P_{j_n}(w_n) P_k(\sharp))_j \cdot \\
& & (\pi_0 P_{j_1}(w_1) \cdots P_{j_n}(w_n) P_k(\sharp))_j^* \\
& = & \sum_{r_k\in F, j_1,\dots,j_n} ||\pi_0 P_{j_1}(w_1) \cdots P_{j_n}(w_n) P_k(\sharp)||^2 \\
& = & p_A(w_1 \cdots w_n)
\end{array}$$

Observe that $P(c) := \sum_j P_j(c) \otimes P_j(c)^*$ is Hermitian and idempotent, hence it is a projector. Observe further that $||\xi|| = ||\pi_0 \cdot \pi_0^*|| = ||\pi_0|| \cdot ||\pi_0|| = 1$ and $||\eta|| = ||\varphi(I) \cdot \sum_{r_k\in F} P_k(\sharp) \otimes P_k(\sharp)^*|| \leq ||\varphi(I)|| = \sqrt{m}$. $\square$

A.2 Proof of Proposition 3

The class $\mathbf{PMO}(\Sigma)$ is closed under the operations of Hadamard product and f-complement.

Proof. Let A, A' be two MON-1QFAs $A = \langle \Sigma \cup \{\#\}, (O_c)_{c\in\Sigma\cup\{\#\},\pi,F}\rangle$ and $A' = \langle \Sigma\cup\{\#\}, (O'_c)_{c\in\Sigma\cup\{\#\},\pi',F'}\rangle$. Without loss of generality, we assume that $V(O_c \otimes O'_c) = V(O_c) \otimes V(O'_c)$ for all $c \in \Sigma \cup \{\#\}$. Let us consider the automaton

$$A'' := \langle \Sigma \cup \{\#\}, (O_c \otimes O'_c)_{c\in\Sigma\cup\{\#\}}, \pi \otimes \pi', F \times F'\rangle$$

For any $w \in \Sigma^*$, by induction on the length $n := |w|$ and the basic property that $(A \otimes B)(C \otimes D) = AC \otimes BD$, we see that $\sigma''(w) = \sigma(w) \otimes \sigma'(w)$, for all $w \in \Sigma^*$. Hence the following holds true for every $w \in \Sigma^*$:

$$\begin{aligned}
p_{A''}(w) &= \mathrm{Tr}\Big(\textstyle\sum_{(r_j,r'_k)\in F\times F'}(P_{r_j}(\#) \otimes P'_{r'_k}(\#))\sigma''(w)(P_{r_j}(\#) \otimes P'_{r'_k}(\#))\Big)\\
&= \mathrm{Tr}\Big(\textstyle\sum_{r_j\in F}\sum_{r'_k\in F'} P_{r_j}(\#)\sigma(w)P_{r_j}(\#) \otimes P'_{r'_k}(\#)\sigma'(w)P'_{r'_k}(\#)\Big)\\
&= \mathrm{Tr}\Big(\Big[\textstyle\sum_{r_j\in F} P_j(\sharp)\sigma(w)P_j(\sharp)\Big] \otimes \Big[\sum_{r'_k\in F} P_{r'_k}(\sharp)\sigma'(w)P_{r'_k}(\sharp)\Big]\Big)\\
&= p_A(w) \cdot p_{A'}(w)
\end{aligned}$$

and this proves closure under Hadamard product. To prove closure under complement, let B the MON-1QFA defined to be equals to the MON-1QFA A but with $V(O^B_\#) := V(O^A_\#) \setminus F_A$. Then $p_B(w) = 1 - p_A(w)$ for every $w \in \Sigma^*$. □

A.3 Proof of Proposition 4

Let $L \in \mathbf{LMO}(\Sigma)$ and χ_L be its characteristic function. For any $\epsilon > 0$, there exists $\phi \in \mathbf{PMO}(\Sigma)$ such that $|\phi(w) - \chi_L(w)| < \epsilon$, for all $w \in \Sigma^*$.

Proof. Let $L \in \mathbf{LMO}(\Sigma)$ and let $A = \langle \Sigma \cup \{\sharp\}, (O_c)_{c\in\Sigma\cup\{\sharp\}}, \pi_0, F\rangle$ be a MON-1QFA over Σ inducing a probabilistic event p_A such that $L = \{w \in \Sigma^* | p_A(w) > \lambda\}$ for some $\lambda \in [0, 1)$ and there exists $\delta > 0$ such that, for all $w \in \Sigma^*$ it holds $|p_A(w) - \lambda| \geq \delta$. Then fix an integer $N \in \mathbb{N}_0$. Without loss of generality, for every $c \in \Sigma \cup \{\sharp\}$, we can define new observables $O_c^{(1)}, \ldots, O_c^{(N)}$ such that $O_c^{(i)}$ possesses the same set of projectors as O_c but different eigenvalues, so that $V(O_c^{(1)} \otimes \cdots \otimes O_c^{(N)}) = V(O_c^{(1)}) \times \cdots \times V(O_c^{(N)})$. Moreover, for $1 \leq i \leq N$, let $F^{(i)}$ be the set of results of $O_\sharp^{(i)}$ corresponding to results of $O_\sharp$ in F. Then, the MON-1QFA $A^{(i)} = \langle \Sigma \cup \{\sharp\}, (O_c^{(i)})_{c\in\Sigma\cup\{\sharp\}}, \pi_0, F^{(i)}\rangle$ over Σ satisfies $p_{A^{(i)}} = p_A$. Now, consider the MON-1QFA over Σ defined as follows

$$A_N = \langle \Sigma \cup \{\sharp\}, (O_c^{(1)} \otimes \cdots \otimes O_c^{(N)})_{c\in\Sigma\cup\{\sharp\}}, \pi_0 \otimes \cdots \otimes \pi_0, F_N\rangle$$

where $(r_{j_1}^{(1)}, \ldots, r_{j_n}^{(N)})$ belongs to F_N if and only if there exist at least λN indexes $i \in \{1, \ldots, N\}$ such that $r_{j_i}^{(i)} \in F^{(i)}$. Then it holds that

$$p_{A_N}(w) = \sum_{k\geq\lambda N} \binom{N}{k} p_A^k(w)(1 - p_A(w))^{N-k} = \Pr\Big[\frac{\sum_{i=1}^N X_i}{N} \geq \lambda\Big]$$

for every $w \in \Sigma^*$, where X_i's are i.i.d. random variables over $\{0,1\}$ with $\Pr(X_i = 1) = p_A(w)$. If $w \notin L$, then $p_A(w) \leq \lambda - \delta$. Thus by Höffdings' inequality, it holds that

$$\Pr\Big[\frac{\sum_{i=1}^{N} X_i}{N}\Big] \leq \Pr\Big[\frac{\sum_{i=1}^{N} X_i}{N} - p_A(t) \geq \delta\Big] \leq e^{-2\delta^2 N}$$

so we get $p_{A_N}(w) \leq e^{-2\delta^2 N}$. If $w \in L$, by the same reasoning we obtain $p_{A_N}(w) \geq 1 - e^{-2\delta^2 N}$. This imply that for any $\epsilon > 0$, for every N such that $\epsilon \geq e^{-2\delta^2 N}$, we have $|\chi_L(w) - p_{A_N}| \leq \epsilon$, where χ_L is the characteristic function of L. ☐

A.4 Proof of Lemma 1

Given a formal series $\phi : \Sigma^* \to [0,1]$, let $\langle \xi, (P(c))_{c\in\Sigma}, \eta\rangle$ be a linear representation of ϕ, where $||\xi|| = 1$ and $P(c)$ is a projector for $c \in \Sigma$, $P(\epsilon) = I$. Suppose that $|\phi(w) - \lambda| \geq \delta > 0$ for all $w \in \Sigma^*$, and let $L := \{w \in \Sigma^* | \phi(w) > \lambda\}$.

(i) T is a regular language on Σ^*.

(ii) there exists a finite state automaton $\langle \Sigma, Q, (\underline{\delta}_c)_{c\in\Sigma}, q_0, F\rangle$ recognizing L such that, for any $w, u \in \Sigma^*$, the following holds: $\underline{\delta}_w(q_0) \neq \underline{\delta}_u(q_0)$ implies $||\xi P(w) - \xi P(u)|| \geq \frac{\delta}{||\eta||}$.

Proof. The proof technique is classical and it is almost identical to the one given in [5] for formal series over $\mathrm{FI}(\Sigma, E)$. Consider the automaton B whose (possibly infinite) state set is $\overline{Q} := \{\xi P(w) | w \in \Sigma^*\}$, the transition on $c \in \Sigma$ is $\overline{\delta}_c(\xi P(w)) := \xi P(wc)$, the initial state is ξ and the set of final states is $\overline{F} := \{\xi P(w) | \xi P(w)\eta^T > \lambda\}$. Then $w \in L$ if and only if $\overline{\delta}(\xi, w) \in \overline{F}$. Now define the binary relation $\sim \subseteq \overline{Q} \times \overline{Q}$ as $\xi P(w) \sim \xi P(u)$ if and only if there exists $x_1, \ldots, x_M \in \Sigma^*$ such that $x_1 = w, x_M = u$ and $||\xi P(x_{i+1}) - \xi P(x_i)|| \leq \frac{\delta}{||\eta||}$ for every $1 \leq i < M$. Since $P(c)$'s are a projectors, they can only decrease distances, then $\sim$ is a congruence. Consider automaton $B/\sim$, this automaton recognizes L. Also, for any $w, u \in \Sigma^*$, $[\xi P(w)]_\sim \neq [\xi P(u)]_\sim$ imply $||\xi P(w) - \xi P(u)|| \geq \frac{\delta}{||\eta||}$ and this proves the inequality stated in (ii). The cardinality of Σ^* is denumerable, for $i \in \mathbb{N}$ let w_i be the representative of the i-th equivalence class $[\xi P(w_i)]$. Observe that the $\xi P(w_i)$'s lie inside the sphere of radius 1, which is a compact set, but if $i \neq j$ then $||\xi P(w_i) - \xi P(w_j)|| \geq \frac{\delta}{||\eta||}$. This means that there are a finite number of equivalence classes of $\sim$, since otherwise they breach the unitary sphere. The thesis follows. ☐

A.5 Proof of Lemma 2

Let Σ be a finite non-empty set. The class $\mathbf{LMO}(\Sigma)$ is closed under intersection, complement and union.

Proof. The proof is almost identical to the one given over (Σ, E) in [5]. Let $L_1, L_2 \in \mathbf{LMO}(\Sigma)$. By Proposition 4 there are $\phi_1, \phi_2 \in \mathbf{PMO}(\Sigma)$ such that $|\phi_1(w) - \chi_{L_1}(t)| < \frac{1}{4}$ and $|\phi_2(w) - \chi_{L_2}(w)| < \frac{1}{4}$, for all $w \in \Sigma^*$. By Proposition 3, $\phi_1 \odot \phi_2 \in \mathbf{PMO}(\Sigma)$. The probabilistic event $\phi_1 \odot \phi_2$, with isolated cut point $\frac{1}{2}$, defines the language $L_1 \cap L_2$. Moreover, $\mathbf{1} - \phi_1 \in \mathbf{PMO}(\Sigma)$ and the complement L_1^c is defined by $\mathbf{1} - \phi_1$ with isolated cut point $\frac{1}{2}$. Therefore $\mathbf{LMO}(\Sigma)$ is a boolean algebra. □

A.6 Proof of Proposition 5

$\mathbf{LMO}(\Sigma)$ is a boolean algebra of regular languages in Σ^* with finite variation. In particular, if L is a language recognized by a MON-1QFA over Σ with m states and isolation δ, then $\sup_{x \in \Sigma^*} \mathrm{var}_L(x) \leq \frac{m}{\delta^2}$.

Proof. The proof is almost identical to the one given over (Σ, E) in [5]. Combining Lemma 1 with Lemma 2, $\mathbf{LMO}(\Sigma)$ is a is a boolean algebra of regular languages. Now, let $L \in \mathbf{LMO}(\Sigma)$, there exists a cut-point λ, a real $\delta > 0$ and a MON-1QFA over Σ, let denote it by $A = \langle \Sigma \cup \{\sharp\}, (O_c)_{c \in \Sigma \cup \{\sharp\}}, \pi_0, F \rangle$, with m pure states such that $L = \{w \in \Sigma^* | p_A(w) > \lambda\}$ and $|p_A(w) - \lambda| \geq \delta$ for all $w \in \Sigma^*$. By Proposition 2 there exists a linear representation $\langle \xi, (P(c))_{c \in \Sigma}, \eta \rangle$ of p_A, where $||\xi|| = 1, P(c) \in \mathbb{C}^{m^2 \times m^2}$ is a projector for every $c \in \Sigma$ and $||\eta|| \leq \sqrt{m}$. By Lemma 1, there exists an automaton recognizing L satisfying the following property: for any $w, u \in \Sigma^*$, if $\underline{\delta}_w(q_0) \neq \underline{\delta}_u(q_0)$ then $||\xi P(w) - \xi P(u)|| \geq \frac{\delta}{||\eta||}$. As a consequence, by considering the minimum automaton $\langle \Sigma, Q, \overline{\delta}, q_0, F \rangle$ for L, we have:

$$\overline{\delta}(q_0, w) \neq \overline{\delta}(q_0, u) \text{ implies } ||\xi P(w) - \xi P(u)|| \geq \frac{\delta}{||\eta||}$$

Since $P(c)$ is a projector, we have $||\xi P(w)||^2 = ||\xi P(wc)||^2 + ||\xi P(w) - \xi P(wc)||^2$, for all $w \in \Sigma^*$. Therefore, if $\delta(q_0, w_1 \cdots w_{k-1}) \neq \delta(q_0, w_1 \cdots w_k)$ for w_i's in Σ, then it follows that:

$$\begin{array}{rcl} ||\xi P(w_1 \cdots w_k)||^2 & = & ||\xi P(w_1 \cdots w_{k-1})||^2 - ||\xi P(w_1 \cdots w_{k-1}) - \xi P(w_1 \cdots w_k)||^2 \\ & \leq & ||\xi P(w_1 \cdots w_{k-1})||^2 - \frac{\delta^2}{||\eta^2||} \\ & \leq & ||\xi P(w_1 \cdots w_{k-1})||^2 - \frac{\delta^2}{m} \end{array}$$

By iterating this way, the following holds

$$0 \leq ||\xi P(w_1 \cdots w_k)||^2 \leq ||\xi||^2 - \mathrm{var}_L(w_1 \cdots w_k) \frac{\delta^2}{m} = 1 - \mathrm{var}_L(w_1 \cdots w_k) \frac{\delta^2}{m},$$

This imply $\mathrm{var}_L(w_1 \cdots w_k) \leq \frac{m}{\delta^2}$, for all $w_1 \cdots w_k \in \Sigma^*$. □